

EXHIBIT 10

4/23/15

AUDIO FRAUD DETECTION

Fraudulent audio tracks can include: illegal use of samples, unauthorized covers, or the upload of material for which the contributor does not have sufficient rights.

Rough estimate of fraudulent/sampled tracks contributed = 10% of submissions, mainly from Ukrainian or Russian IPs.

While our curators are working to detect fraudulent tracks with moderate success, we need a technology enabled and scalable solution implemented. Currently the tools we are using are ID and location/IP/Cookie verification, and Shazam (a consumer app) on a manual basis.

Most importantly, we need to demonstrate that we are doing due diligence to detect and remove this content. While we've been successful at filtering most of it, we have already faced legal threats from competitors for exclusive tracks they represent which have gotten through our curators, and are likely to encounter these issues increasingly as we scale.

Solutions.

There are two major systems of content identification used in audio. YouTube/Google have their own proprietary Content ID system, which does not have a public API available. The competing content identification system is called Audible Magic, which is used by the other major UGC networks, including Facebook, Soundcloud, and Vimeo.

We have a test license already in place for Audible Magic (purchased for \$_____ in _____, expires May 2015).

While the technology isn't perfect (our test showed it was only capable of identify non-modified samples at least 30 seconds in length), it is industry standard, and may suffice for providing due diligence should a fraudulent item pass through our curatorial wall.

This would not necessarily preclude the use of additional services, but seems a likely minimum viable solution.

Workflow:

- Track is submitted
- Track "scanned" for sonic matches (samples, recognizable sounds)
- "Red flagged" (potentially fraudulent) tracks are pulled aside, placed in own queue so as to not disrupt curating process
- "Red flagged" tracks are later double-checked for fraud manually

A back-log scrub of the library is also crucial in order to remove potentially fraudulent tracks still online.

CONTENT AUDIT: REDUCING RISK IN THE COLLECTION

POND5 H1 STRATEGIC GOALS:

- Enterprise Sales
- Improving Quality of Licensable Collection
- Artist Fraud Protection & Onboarding Workflow (Artist ID+)
- Legal Risk Abatement

Prospective corporate customers sometimes need to feel secure in the licensability of the Content they license and occasionally request that Pond5 indemnify them against copyright infringement or violation of privacy / publicity rights based on the customer's use of the content and to vastly increase limits of liability under those indemnities. Following are our proposals to mitigate the increased risks of accommodating such demands. These steps would be essential maintaining our reputation for having quality content.

BACKGROUND:

While our Content License Agreement is clear about the IP risks of licensing content and transfer such risk to the buyer, reputational and residual legal risks remain apparent. Our goal is to make it possible for all contributors to safely provide content to re-license; we want to add more content, not less and expand the universe, and make the Pond5 environment more attractive for contributors and customers.

What Pond5 needs to know from our contributors to minimize risk:

1. Is the Pond5 contributor "real?"

- **Current Process:** Video/Photo Curators review photo ID only
- **Problems:**
 - Time-consuming - curator manpower - takes away from curating
 - Ineffective - photo ID's from disparate countries are difficult to assess

- ☐ Operational inefficiency - unscalable and not our core competency
 - ☐ Frustrated contributors due to extended wait times for verification
 - ☐ If curators cost \$25/hour and can process 100 IDs over 8 hours, it costs P5 \$2.00 per photo ID-only verification or 1K per week.
- **Goal:** Thorough, efficient vetting process that allows us to feel comfortable with both contributors and content
- **Risks:**
 - ☐ Allowing fraudsters onto site due to ineffective / incomplete verification (which has happened recently on the SFX side - e.g. Hempton lawsuit)
 - ☐ Irrate contributors over wait times (check forums)
 - ☐ Loss of potential revenue and content
- **Criteria:**
 - ☐ "Digital Identity" verification / match
 - ☐ IP / physical address match
 - ☐ Official website or LinkedIn page with connections
 - ☐ Passport / photo ID, physical address, phone #, Company Tax ID
 - ☐ Licensing / Billing info **required** for User Info
- **Recommendation:** The current system of solely looking at a passport isn't as efficient as we'd like it to be. We need additional info besides Photo ID to determine if the contributor is real. We can either invest company/curator time in looking at other forms ID or we use a third-party solution, such as:

Socure: "digital identity" solution that assigns specific attributes (email, mobile phone, social/non-social presence) different scores. 6 second verification time. 12K/year

NetVerify: a "Know Your Customer" solution that scans photo ID and compares a face match (along with "human document review specialist" helping out). Using a non-Product intensive redirect link our curators could check previous NetVerify verifications, or access database with results.

Verification time is 4 minutes. Currently their software can't read Cyrillic.
37K/year

VerifyMe: a "device solution" that combats fraud and identity theft using physical, cyber (geo-location) and biometric security solutions. They insure that the person logging in is the person who signed up.

Trulioo: a "data solution" that matches specific attributes (name, address, phone number) to an online profile (based off of credit bureau info, etc). Limited in terms of the number of countries they serve.

2. Is our contact the Pond5 contributor listed above?

- **Current Process:** Video / Photo Curators review photo ID, IP origin location and check for cookie matches, but there's no way to know for sure
- **Problem:**
 - We may confirm a company is "real," but our contact could be someone impersonating that company with a different address or URL (example, user: ckennedy342). We're not matching physical address to IP or geo-location of the actual company the entity we're dealing with claims to be.
- **Goal:** Ensure our contact is with the legitimate organization or artist they say they are.
- **Risks:**
 - Copyright infringement
 - Irrate contributors
 - Identity theft
- **Criteria:**
 - "Digital Identity" verification / match

OPTION 1: The contributor is the artist / copyright owner

This is the ideal scenario (**lowest risk**).

OPTION 2: The contributor is an authorized representative of the artist

- If they're an employee of company / corporation (lower risk)...
We need to confirm this person has authority
- If they're the Licensing agent (higher risk)...
Proof / license of authorization?
- If they're the authorized distributor (higher risk)...
Proof of authorization?

We need to know the contributor actually exists and has the authorization to provide us content.

3. Does the contributor have the right to license the work they're submitting?

- **Current Process:** We don't ask for any proof of license.
- **Problem:**
 - Contributors may have acquired collection, but we don't know if they have any legal rights to do so.
 - Contributors buy accounts (TheEngineer) ranging from legit to wildly sketchy
- **Goal:** Ensure each batch of content is safe and vetted
- **Risks:**
 - Copyright infringement
 - Legal complications
 - Irrate contributors
- **Criteria:**
 - Bill of Sale and Transfer of Ownership should exist
 - Review substance and reputation of contributor

- Senior Level Review - some combination of # of employees, years in business, D&B credit report, E&O insurance

Recommendation:

- Process: **BASED ON THE DMCA, THE MORE WE DO IN AN AUTOMATED FASHION THROUGH THE PLATFORM ITSELF (AND THE LESS HUMAN INTERACTION), THE MORE WE'RE COVERED. MORE VERIFICATION OF ARTIST. HAVING CONTROL OVER CONTENT IS THE ISSUE**
- It's not just what you do, but what you say publicly
- Some form of content-matching should be part of the process (YouTube ContentID admin via AdRev)
- Divide library content into categories based on content origin

RISK

- In past three years we've had a handful of cases where we've received notices of infringement which have generally been resolved amicably by removing the content in good faith. The costs have been significant primarily in the form of internal staff time and some legal fees.
- We're not licensing *Star Wars*, we're lower risk, lower cost stock items of which a good portion have no third-party rights or releases required (shots of the moon, sea, production elements, etc.).
- The majority of our issues to this point have involved fraud and content stolen from other Pond5 contributors.

Our job is to find a scalable automated solution that decreases the risk that the acquired content not licensable. The reality is that Pond5 has faced very few inquiries licensing tens of thousands of items over the past decade. We're hoping to encourage all types of contributors - aggregators, agents, production companies, bands, graphics houses, talent and other rights holders- to submit content, but we want to make sure risk continues to be minimized across the board. Here are some recommendations on how to continue that:

OPTION 1: "FastTrack"

Pond5 determines an artist has substantial assets, reputation, insurance, or some combination (*dependent on size of company (number of employees, revenue, time in business, E&O up to 1 million, making Pond5 named insured,) then all of their content passes through to pre-approved state without batch review. "FastTrack" serves as both an integrity check and gives us more info to assess if the contributor is honest.

OPTION 2: Content Tiering

Pond5 makes a determination that certain content has a lower threshold because the legal risks are lower.

Self-produced contributor content by contributors with low-risk subject matter (nature, elements) could move through queue quicker and achieve clearance.

OPTION 3: Contributor Provides More Documentation

- Acquired content (for select categories)
- Repped Content (for select categories)

OPTION 4: Upload page and process involves asking Contributor for more info (see examples)

RELEASES

- **Current Process:** Accept release with photo & witness signature
- **Problem:** Is witness optional?
- **Goal:** Consistent release protocol
- **Risks:** Improperly released and/or unreleased content makes it onto the site
- **Criteria:** Model photo / witness signature?
- **Recommendation:** Our upload standards should be at least the same or better than our competitors, and rewritten to include revisions (take out anything indicating control over content, ie "reviewing" Curator Checklist for existing releases for video/photos, revised model & property releases + EZ release for download on Pond5). See Curator Checklist.

MODEL RELEASE - ADULT / MINOR

- Individual picture for person required
- Witness signature? - Optional (we shouldn't be stricter than Getty), while Simon is pro-witness. We need to be more secure and we've been asking for witness signatures for a while because we can't do model verification.
 - **No legal basis for required witness signature in the U.S.**
- Model Release and Editorial?
 - Model release but no property release could count as Editorial
- [EZ Release](#) - \$10 smartphone app, allows contributor to create model / property releases with photos and signatures (Approved by the leading stock photo agencies: [Getty Images](#), [iStockPhoto](#), [Shutterstock](#), [BigStock](#), [Dreamstime](#), Alamy and others)
- In 2015, Pond5 sold five releases to clients at \$50 per release (\$75 for non-P5 releases)

PROPERTY RELEASE

- Property Releases are meant to cover two situations:
 - identifying house/privacy publicity
 - any item where there is something copyrighted/trademarked

TRADEMARK RELEASE

- Release needed from owner of trademark, legal protection for us

CA PRIVACY LANGUAGE ISSUE

- Current CA language: buyer's job to confirm that the right releases have been obtained (even though we say we have a model release).
- If we indemnify, we may need to change the language and then we lose that "out."

CONTEXT ISSUE

- We warrant that the release will not violate privacy or publicity but we're indemnifying for **how** the content is used.

EDITORIAL

- **Current Process:** Curators mark any shot with unreleased, recognizable features, logos, or sensitive elements as "Editorial"
- **Problem:** Editorial Content cannot be indemnified
- **Goal:** Consistent Editorial protocol
- **Risks:** Content incorrectly labeled - or not labeled - editorial could be present legal complications
- **Criteria:** Newsworthy?
- **Recommendation:**

What is "editorial?"

- Crowd shots - people unaware of being filmed, even though they're in public areas- recognizable figures - we need a list/guidelines
- Property issue - public vs. private, copyrighted designs, buildings, logos, license plates, cars, **NO ADVERTISING**
- Who can use editorial content?
- Only curators can mark as editorial via Edit Item page
- Potentially 15 % of video content is marked editorial
- How often is editorial content purchased?
- Exploitation and nudity - it's the curator's call to make and/or reject
- Cryan: it's needs to be newsworthy, current
- Does Shutterstock indemnify any editorial content?

MORAL RIGHTS

If you're part of the creative process, your rights carry wherever that content goes, irregardless of who owns it

- International law - not in US
- What you can and can't do

ARTIST FRAUD PROTECTION

How does each media type currently handle fraud? (link)

- **Current Process:** Dependent on media type
- **Problem:** Potentially inefficient, needs constant revisions
- **Goal:** Vetted, clean media collection
- **Risks:** Legal and reputational damage
- **Criteria:** What do we need to feel comfortable with the contributors and their content?

AUDIO (MUSIC)

- Require a couple of individual “stem” tracks (single instruments) for each track - will prevent fraudsters and act as an upsell opportunity for artists while expanding their portfolios and giving buyers more options
- Quarterly Audible Magic processing
- Individual Shazam spot-checking as test of third-party tools
- Cross-reference with internal documentation

AUDIO (SFX)

- In-house duplication detection coupled with extensive vetting process (listed above) and “approved” SFX contributors’ list

VIDEO

- Require video sequences?
- entire shoot uploads?
- track file comparison (currently not automated - not effective)
- track DMCA notices - only applies to copyright infringement, potentially inaccurate (Javi, David)

PHOTO

- tineye.com

ILLUSTRATIONS / PSDs

- tineye.com
- vector layers

AE

- Jobert: *It's very hard to determine fraud for After Effects files. Because there's no "Shazam" for AE. Also if ever I need to investigate I would need to have the capacity to buy from our competitors in order to compare the project files of the said fraudulent files. Assuming that the complain is a stolen AE template.*

3D

-

CLEARED CONTENT

- **Current Process:** AdRev unofficially releases ContentID claims in conjunction with CS team
- **Problem:** Short-term revenue left on table, contributors get monies owed to them
- **Goal:** Streamlined YouTube ContentID registration and admin via AdRev
- **Risks:** Could alienate some contributors
- **Criteria:** Composers who *do not* have their music already engaged with *distributors, aggregators, labels or existing fingerprinting platforms* in the first place

YOUTUBE CONTENT ID

- AdRev is an administrative service that protects and monetizes copyright usage on YouTube
 - Short-term revenue generating opportunity as well as a post-curation layer of protection
 - P5 contributor opts in content to AdRev for YouTubeContentID admin - 80% of monetization goes to contributor, 10% to AdRev, 10% to Pond5.
 - AdRev scans ALL YT videos (regardless of upload date) and will begin monetization from that point forward.
 - Other libraries of our scope and size are in this 6 to 7 figure range. Current CPM on claimed content for SR claims is around \$.30 / 1,000 views.